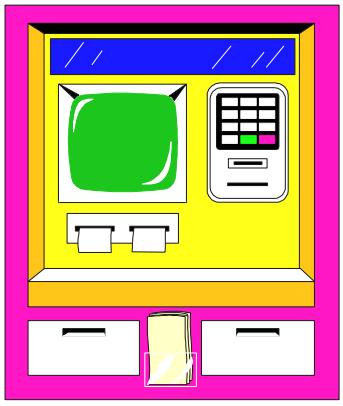
WHAT IS ELECTRONIC BANKING?



A mini-lesson for:

secondary school teachers

adult and community educators

students and consumers

This mini-lesson includes learning objectives, background information, discussion questions, activities, a worksheet and sources of additional information.

OBJECTIVES

Learners will:

- define electronic banking.
- describe several electronic fund transfer services.
- compare several types of electronic currency.
- list consumer protections under the Electronic Funds Transfer Act.

Electronic Banking

Electronic banking, also known as electronic funds transfer (EFT), is simply the use of electronic means to transfer funds directly from one account to another, rather than by check or cash. You can use electronic funds transfer to:

- have your paycheck deposited directly into your bank or credit union checking account.

- withdraw money from your checking account from an ATM machine with a personal identification number (PIN), at your convenience, day or night.
- instruct your bank or credit union to automatically pay certain monthly bills from your account, such as your auto loan or your mortgage payment.
- have the bank or credit union transfer funds each month from your checking account to your mutual fund account.
- have your government social security benefits check or your tax refund deposited directly into your checking account.
- buy groceries, gasoline and other purchases at the point-of-sale, using a check card rather than cash, credit or a personal check.
- use a smart card with a prepaid amount of money embedded in it for use instead of cash at a pay phone, expressway road toll, or on college campuses at the library's photocopy machine or bookstores.
- use your computer and personal finance software to coordinate your total personal financial management process, integrating data and activities related to your income, spending, saving, investing, recordkeeping, bill-paying and taxes, along with basic financial analysis and decision making.

Automated Teller Machines (ATMs) also called 24-hour tellers are electronic terminals which give consumers the opportunity to bank at almost any time. To withdraw cash, make deposits or transfer funds between accounts, a consumer needs an ATM card and a personal identification number. Some ATMs charge a usage fee for this service, with a higher fee for consumers who do not have an account at their institution. If a fee is charged, it must be revealed on the terminal screen or on a sign next to the screen.

Direct Deposit and Withdrawal Services allow consumers to authorize specific deposits, such as paychecks or social security checks, to their accounts on a regular basis. It is also possible to authorize the bank, for a fee, to withdraw funds from your account to pay your recurring bills, such as mortgage payment, installment loan payments, insurance premiums and utility bills.

Pay by Phone Systems let consumers phone their financial institutions with instructions to pay certain bills or to transfer funds between accounts.

Point-of-Sale Transfer Terminals allow consumers to pay for retail purchase with a **check card**, a new name for debit card. This card looks like a credit card but with a significant difference— the money for the purchase is transferred immediately from your account to the store's account. You no longer have the benefit of the credit card "float", that is the time between the purchase transaction and when you pay the credit card bill. With immediate transfer of funds at the point-of-sale, it is easy to overdraw your checking account and incur additional charges unless you keep careful watch on spending.

Personal Computer Banking Services offer consumers the convenience of conducting many banking transactions electronically using a personal computer. Consumers can view their account balances, request transfers between accounts and pay bills electronically from home.

Types of Electronic Currency

Check Cards, the new name for debit cards, can be used instead of cash, personal checks or credit cards. As stated, when you use a check card you transfer funds immediately from your account to the store's account. A growing number of consumers use check cards because they eliminate the hassle and risks of writing checks or carrying large amounts of cash. Important facts you need to know are:

- You have less bargaining power with a check card than with a credit card. With a credit card you have the right to refuse to pay for the purchase if you are not satisfied. With a debit card you have already paid for the product, so you have less bargaining power with the merchant.

- A thief with your check card and PIN number can take all the money in your account. The thief can even make point-of-sale purchases without your PIN.

- Your liability is limited to $50 if you report the checkcard loss within two days, any longer and your liability can go to $500. After 60 days, you can be responsible for the entire amount.

Note: MasterCard and Visa have voluntarily capped the loss liability of checkcard holders at $50. "As welcome as these voluntary protections are, they are too important to be left to the kindness of bank marketing departments," writes **Consumer Reports**. The consumer advocacy magazine advocates federal law changes to make consumer liability caps mandatory.

- In an era of increasing bank fees, consumers can expect to pay for the service of using a checkcard.

- It is the consumer's responsibility to keep checkcard receipts and deduct the dollar amounts of the purchase from your bank balance immediately, in order to avoid overdraft changes.

Smart Cards, sometimes called stored-value cards, have a specific amount of credit embedded electronically in the card. For example, a $100 smart card that you have purchased in advance can be used to cover expenses such as pay phone charges, bridge or expressway tolls, parking fees or Internet purchases. These cards make the transaction fast, easy and convenient.

Smart card technology is in a period of rapid change. Ultimately consumers should be able to customize their smart cards to suit their financial needs with access from their personal computer or cellular phone. Some important consumer issues are:

- Smart cards are the equivalent of cash so must be guarded.

- Procedures for recovering the value of a malfunctioning smart card are unclear.

- The computer chip within the card will contain both financial and personal information. Privacy and security issues could be a problem.
-

Smart cards may not be covered by the Electronic Funds Transfer Act in case of loss or misuse of the card.

Digital Cash is designed to allow the consumer to pay cash rather than use a credit card to purchase products on the Internet. One type of digital cash allows consumers to transfer money from a financial institution or a credit card into an "electronic purse". The cash is held in a special bank account that is linked to your computer. Another type of digital cash converts money into digital coins that can be placed on your computer's hard drive.

Digital checks allow consumers to use their personal computers to pay recurring bills. Consumers can use computer software provided by a bank, or they can use personal finance software packages such as Quicken or Microsoft Money and subscribe to an electronic bill-paying service.

The technology of paying bills electronically by home computers is advancing rapidly, but relatively few businesses currently can accept payments made directly by computers. Digital checking is expensive. Fees generally run from $5 to $10 a month for 20 transactions. Privacy and security issues are major consumer concerns. Encryption technology may lessen privacy concerns in the future.

Consumer Protection -- Electronic Funds Transfer Act

The 1978 Electronic Funds Transfer Act is the governing statute while the Federal Reserve Board's Regulation "E" provides guidelines on electronic funds transfer card liability. The regulations require that:

- a valid EFT card can be sent only to a consumer who requests it.
- unsolicited cards can be issued only if the card cannot be used until validated.
- the financial institution must inform you of your rights and responsibilities under the law in a written **Disclosure Statement**, including the procedure to correct errors in your periodic statements.
- the user is entitled to a written receipt when making deposits or withdrawals from an ATM or using a point-of-sale terminal to make a purchase. The receipt must show the amount, date and type of transfer.
- periodic statements must confirm the amount of all transfers, the dates and types of transfers, type of accounts to or from which funds were transferred, and the address and phone number to be used for inquiries regarding the statement.

Problems and Errors. You have 60 days from the date a problem or error appears on your written terminal receipt or on your periodic statement to notify your financial institution. If you fail to notify the financial institution of the error within 60 days, you may have little recourse. Under federal law, the financial institution has no obligation to conduct an investigation if you have missed the 60-day deadline.

Lost cards. If you report an ATM or EFT card missing before it is used without your permission, the card issuer cannot hold you responsible for any unauthorized withdrawals. If unauthorized use occurs before you report it, the amount you can be held responsible for depends upon how quickly you report the loss. If you report the loss within two business days after you realize the card is missing but you do report its loss within 60 days after your statement is mailed to you, you could lose a much as $500 because of an unauthorized withdrawal.

If you do not report an unauthorized withdrawal within 60 days after your statement is mailed, you risk losing all the money in your account plus the unused portion of your maximum line of credit established for overdrafts.

See our Web Sites:

ATMs http://www.dfi.state.in.us/conscredit/atms.htm	**Credit & ATM Cards - What to do if They're Stolen** http://www.dfi.state.in.us/conscredit/stolen atm.htm	**Cyber Shopping** http://www.dfi.state.in.us/conscredit/Cybersh.html
Automatic Debit Scams http://www.dfi.state.in.us/conscredit/AutomScm.html	**Credit and ATM Cards** http://www.dfi.state.in.us/conscredit/CrATM.html	
Debit Cards vs. Credit Cards http://www.dfi.state.in.us/conscredit/debit_vs.htm	**Electronic Banking** http://www.dfi.state.in.us/conscredit/ebk.htm	**Fraud on the Internet** http://www.dfi.state.in.us/conscredit/FRAUDint.htm

DISCUSSION TOPICS

1. List several examples of electronic funds transfers and discuss your experiences with EFTs.

2. Describe smart cards and give examples of what they can do.

3. Describe check cards and give examples of what they can do.

4. What consumer protections apply to lost or stolen EFT cards under the federal Electronic Funds Transfer Act?

5. What information must be included in periodic EFT statements from your financial institution, and why is it important for consumers to check this information for accuracy as soon as possible after receipt?

ACTIVITY

1. Invite a resource person from a local bank or credit union to come to your classroom to explain their EFT services. Ask about costs, consumer problems, consumer protections under the law, and the resource person's vision of new uses of electronic money in the future.

2. Survey several friends about their experiences with electronic money and their greatest concerns.

3. Using the EFT COMPARISON WORKSHEET (last page), evaluate the EFT services provided by local financial institutions, including costs, benefits and restrictions. Determine which services would suit your financial situation and provide the most convenience and benefits.

Give students our Brochures.

SOURCES OF ADDITIONAL INFORMATION

Articles

Banking: There's No Place Like Home by Kathy Yakal. Kiplinger's Personal Finance Magazine, pp. 61-66, (December 1997).

Check Cards: Should you replace your ATM card? Consumer Reports, pp. 68-69, (October 1997).

Electronic Commerce and The Future of Money; Technology and You, by Tariq K. Muhammad, Black Enterprise, pp. 255-259, (June 1997).

How Will We Pay On The Internet? by James McAndrews, Consumers' Research, pp. 29-33, (April 1997).

Paying Bills By Computer; Time to switch to digital checks? Consumer Reports, pp. 54-55, (August 1997).

What to know before you spend cyberdough, by Ellen Start, Money Magazine, pp. 33-35, (January 1997).

What works and what doesn't in the world of Digital Finance, by Peter Keating, Money Magazine, pp. 135-143, (July 1996).

Lesson Plan

Lesson Plan on Electronic Banking, available free from:

Public Information Center
Federal Reserve Bank of Chicago
P.O. Box 834
Chicago, IL 60690-0834
Telephone: (312) 322-5111

Pamphlets

Available free from:
Board of Governors of the Federal Reserve System
Publications Services
Division of Support Services
Washington, DC 20551

Alice in Debitland
Consumer Handbook to Credit Protection Laws
A Consumer's Guide to Direct Payment
Electronic Banking for Today's Consumer
The Story of Checks and Electronic Payments

Available free from:
MasterCard International
1401 Eye Street, NW
Washington, DC 20005
Telephone: (800) 999-5136

The ATM Cash Card Quiz

Available free from:
Federal Trade Commission
Consumer Response Center
Washington, DC 20580-0001
Telephone: (202) 326-3650
http://www.ftc.gov

Cybershopping: Protecting Yourself When Buying Online Electronic Banking
Lost or Stolen: Credit and ATM Cards

Available free from:
National Consumers League
1701 K Street, NW
Suite 1200
Washington, DC 20006
Telephone: (202) 835-3323

Debit Cards; Beyond Cash & Checks

Available free from
Public Information Center
Federal Reserve Bank of Chicago
P.O. Box 834
Chicago, IL 60690-0834
http://www.frbchi.org

Electronic Money

Available free from:
St. JamesConsumer Information Center - 7D
P.O. Box 100
Pueblo, CO 81002
http://www.pueblo.gsa.gov

Shopping With Your ATM Card

Available free from:
Call For Action Network Office
5272 River Road
Suite #300
Bethesda, MD 20816
Telephone: (800) 647-1756

A Smart New Way to Pay; What Savvy Consumers Need to Know About Debit Cards

Available free from:
Direct Marketing Association
1120 Avenue Of The Americas
New York, NY 10036-6700
Telephone: (212) 768-7277

Tips For Cybershopping

Web Sites

Department of the Treasury, Financial Management Service

Consumer Information Center
A consumer's Guide To the Expanding Uses of ATM cards, Shopping With Your ATM Card

Federal Trade Commission
Electronic Banking (March 1997)

EFT COMPARISON WORKSHEET

Name of the Financial Institution _____

EFT Service	Cost	Benefits	Restrictions

Name of the Financial Institution _____

EFT Service	Cost	Benefits	Restrictions

Selected Services _____

_____

Selected Financial Institution _____

Fraudulent telemarketers have found yet another way to steal your money, this time from your checking account. Consumers across the country are complaining about unauthorized debits (withdrawals) from their checking accounts.

Automatic debiting of your checking account can be a legitimate payment method; many people pay mortgages or make car payments this way. But the system is being abused by fraudulent telemarketers. Therefore, if a caller asks for your checking account number or other information printed on your check, you should follow the same warning that applies to your credit card number -- **do not give out checking account information over the phone unless you are familiar with the company and agree to pay for something**. **Remember**, if you give your checking account number over the phone to a stranger for "verification" or "computer purposes," that person could use it to improperly take money from your checking account.

HOW THE SCAM WORKS

You either get a postcard or a telephone call saying you have won a free prize or can qualify for a major credit card, regardless of past credit problems. If you respond to the offer, the telemarketer often asks you right away, "Do you have a checking account?" If you say "yes," the telemarketer then goes on to explain the offer. Often it sounds too good to pass up.

Near the end of the sales pitch, the telemarketer may ask you to get one of your checks and to read off all of the numbers at the bottom. Some deceptive telemarketers may not tell you why this information is needed. Other deceptive telemarketers may tell you the account information will help ensure that you qualify for the offer. And, in some cases, the legitimate telemarketer will honestly explain that this information will allow them to debit your checking account.

Once a telemarketer has your checking account information, it is put on a "demand draft," which is processed much like a check. The draft has your name, account number, and states an amount. Unlike a check, however, the draft does not require your signature. When your bank receives the draft, it takes the amount on the draft from your checking account and pays the telemarketers' bank. You may not know that your bank has paid the draft until you receive your bank statement.

WHAT YOU CAN DO TO PROTECT YOURSELF

It can be difficult to detect an automatic debit scam before you suffer financial losses. If you do not know who you are talking to, follow these suggestions to help you avoid becoming a victim:

* Don't give out your checking account number over the phone unless you know the company and understand why the information is necessary.
* If someone says they are taping your call, ask why.
* Don't be afraid to ask questions.
* Companies do not ask for your bank account information unless you have expressly agreed to this payment method.

ITS THE LAW

Since December 31, 1995, a seller or telemarketer is required by law to obtain your verifiable authorization to obtain payment from your bank account. That means whoever takes your bank account information over the phone must have your express permission to debit your account, and must use one of three ways to get it. The person must tell you that money will be taken from your bank account. If you authorize payment of money from your bank account, they must then get your written authorization, tape record your authorization, or send you a written confirmation before debiting your bank account.

If they tape record your authorization, they must disclose, and you must receive, the following information:

* The date of the demand draft;
* the amount of the draft(s);
* the payers' name (who will receive your money);
* the number of draft payments (if more than one);
* a telephone number that you can call during normal business hours; and
* the date that you are giving your oral authorization.

If a seller or telemarketer uses written confirmation to verify your authorization, they must give you all the information required for a tape recorded authorization and tell you in the confirmation notice the refund procedure you can use to dispute the accuracy of the confirmation and receive a refund.

WHAT TO DO IF YOU ARE A VICTIM

If telemarketers cause money to be taken from your bank account without your knowledge or authorization, they have violated the law. If you receive a written confirmation notice that does not accurately represent your understanding of the sale, follow the refund procedures that should have been provided and request a refund of your money. If you do not receive a refund, it's against the law.

If you believe you have been a victim of fraud, contact your bank immediately. Tell the bank that you did not okay the debit and that you want to prevent further debiting. You also should contact your state Attorney General. Depending on the timing and the circumstances, you may be able to get your money back.

MORE INFORMATION

To learn more about your rights under the telemarketing Sales Rule and how to protect yourself from fraudulent telephone sales practices, request a free copy of *Straight Talk About Telemarketing*. Contact.

Consumer Response Center
Federal Trade Commission
Washington DC 20580
(202) 326-2222
TDD: (202) 326-2502

* * * * * * * * * * * * *

The Indiana Department of Financial Institutions, Division of Consumer Credit has many other credit related brochures available, such as:

- Answers to Credit Problems
- Applying for Credit
- At Home Shopping Rights
- Bankruptcy Facts
- Buried in Debt
- Car Financing Scams
- Charge Card Fraud
- Choosing A Credit Card
- Co-Signing
- Credit and Divorce
- Credit and Older Consumers
- Deep in Debt?
- Equal Credit Opportunity
- Fair Credit Reporting
- Fair Debt Collection
- Gold Cards
- Hang up on Fraud
- High Rate Mortgages
- Home Equity Credit Lines
- How to Avoid Bankruptcy
- Indiana Uniform Consumer Credit Code
- Look Before you Lease
- Mortgage Loans
- Repossession
- Reverse Mortgage Loans
- Rule of 78s – What is it?
- Scoring for Credit
- Shopping for Credit
- Using Credit Cards
- Variable Rate Credit
- What is a Budget?
- What is the DFI?

Call our toll-free number or write to the address on the cover for a copy of any of the brochures listed or for further consumer credit information. You can also access information at our web site on the Internet: http://www.dfi.state.in.us, then click on Consumer Credit.

Automatic Debit Scams

DEPARTMENT OF FINANCIAL INSTITUTIONS
Consumer Credit Division
402 West Washington Street, Room W066
Indianapolis, Indiana 46204
317-232-3955
1-800-382-4880
Web Site http://www.dfi.state.in.us

What To Do If They're Lost or Stolen

Many people find it easy and convenient to use credit and ATM cards. The Fair Credit Billing Act (FCBA) and the Electronic Funds Transfer Act (EFTA) offer procedures for you and businesses to use if your cards are lost or stolen.

Limiting Your Financial Loss

Report the loss or theft of your credit and ATM cards to the card issuers as quickly as possible. Many companies have toll-free numbers and 24-hour service to deal with such emergencies. It's a good idea to follow up your phone calls with a letter. Include your account number, when you noticed your card was missing, and the date you first reported the loss.

You also may want to check your homeowner's insurance policy to see if it covers your liability for card thefts. If not, some insurance companies will allow you to change your policy to include this protection.

Credit Card Loss. If you report the loss before the cards are used, the FCBA says the card issuer cannot hold you responsible for any unauthorized charges. If a thief uses your cards before you report them missing, the most you will owe for unauthorized charges is $50 per card. This is true even if a thief uses your credit card at an ATM machine to access your credit card account.

However, it's not enough simply to report your credit card loss. After the loss, review your billing statements carefully. If they show any unauthorized charges, send a letter to the card issuer describing each questionable charge. Again, tell the card issuer the date your card was lost or stolen and when you first reported it to them. Be sure to send the letter to the address provided for billing errors. Do not send it with a payment or to the address where you send your payments unless you are directed to do so.

ATM Card Loss. If you report an ATM card missing before it's used without your permission, the EFTA says the card issuer cannot hold you responsible for any unauthorized withdrawals. If unauthorized use occurs before you report it, the amount you can be held liable for depends upon how quickly you report the loss. For example, if you report the loss within two business days after you realize your card is missing, you will not be responsible for more than $50 for unauthorized use.

However, if you don't report the loss within two business days after you discover the loss, you could lose up to $500 because of an unauthorized withdrawal. You risk unlimited loss if you fail to report an unauthorized transfer or withdrawal within 60 days after your bank statement is mailed to you. That means you could lose all the money in your bank account and the unused portion of your line of credit established for overdrafts.

If unauthorized transactions show up on your bank statement, report them to the card issuer as quickly as possible. Once you've reported the loss of your ATM card, you cannot be held liable for additional amounts, even if more unauthorized transactions are made.

Protecting Your Cards

The best protections against card fraud are to know where your cards are at all times and to keep them secure. For ATM card protection, it's important to keep your Personal Identification Number (PIN) a secret. Don't use your address, birth date, phone or social security number. Memorize the number. Statistics show that in one-third of ATM card frauds, cardholders wrote their PINS on their ATM cards or on slips of paper kept with their cards.

The following suggestions may help you protect your credit and ATM card accounts.

For Credit Cards:

- Be cautious about disclosing your account number over the phone unless you know you are dealing with a reputable company.
- Never put your account number on the outside of an envelope or on a postcard.
- Draw a line through blank spaces on charge slips above the total so the amount cannot be changed.
- Don't sign a blank charge slip.
- Tear up carbons and save your receipts to check against your monthly billing statements.
- Open billing statements promptly and compare them with your receipts. Report mistakes or discrepancies as soon as possible to the special address listed on your statement for "billing inquiries." Under the FCBA, the card issuer must investigate billing errors reported to them within 60 days of the date your statement was mailed to you.
- Keep a record — in a safe place separate from your cards — of your account numbers, expiration dates, and the telephone numbers of each card issuer so you can report a loss quickly.
- Carry only those cards that you anticipate you'll need.

For ATM cards:

- Don't carry your PIN in your wallet or purse or write it on your ATM card.
- Never write your PIN on the outside of a deposit slip, an envelope, or on a postcard.
- Take your ATM receipt after completing a transaction.
- Reconcile all ATM receipts with bank statements as soon as possible.

Buying a Registration Service

For an annual fee of $10 to $35, companies will notify the issuers of your credit and ATM accounts if your card is lost or stolen. This service allows you to make only one phone call to report all card losses rather than calling individual issuers. Most services also will request replacement cards on your behalf.

Purchasing a card registration service may be convenient, but it's not required. The FCBA and the EFTA give you the right to contact your card issuers directly in the event of a loss or suspected unauthorized use.

If you decide to buy a registration service, compare offers. Carefully read the contract to determine the company's obligations and your liability. For example, will the company reimburse you if it fails to notify card issuers promptly once you've called in the loss to the service? If not, you could be liable for unauthorized charges.

* * * * * * * * * * * * * *

The Indiana Department of Financial Institutions, Division of Consumer Credit has many other credit related brochures available, such as:

- Answers to Credit Problems
- Applying for Credit
- At Home Shopping Rights
- Bankruptcy Facts
- Buried in Debt
- Car Financing Scams
- Charge Card Fraud
- Choosing A Credit Card
- Co-Signing
- Credit and Divorce
- Credit and Older Consumers
- Deep in Debt?
- Equal Credit Opportunity
- Fair Credit Reporting
- Fair Debt Collection
- Gold Cards
- Hang up on Fraud
- High Rate Mortgages
- Home Equity Credit Lines
- How to Avoid Bankruptcy
- Indiana Uniform Consumer Credit Code
- Look Before you Lease
- Mortgage Loans
- Repossession
- Reverse Mortgage Loans
- Rule of 78s – What is it?
- Scoring for Credit
- Shopping for Credit
- Using Credit Cards
- Variable Rate Credit
- What is a Budget?
- What is the DFI?

Call our toll-free number or write to the address on the cover for a copy of any of the brochures listed or for further consumer credit information. You can also access information at our web site on the Internet: http://www.dfi.state.in.us, then click on Consumer Credit.

CREDIT AND ATM CARDS

DEPARTMENT OF FINANCIAL INSTITUTIONS
Consumer Credit Division
402 West Washington Street, Room W066
Indianapolis, Indiana 46204
317-232-3955
1-800-382-4880
Web Site http://www.dfi.state.in.us

PROTECTING YOURSELF WHEN BUYING ONLINE

With a few key strokes and the click of a mouse you can shop at home from your computer. Sounds great, right? No traffic. No parking problems. No lines or crowds. No hassles with the weather.

Online shopping can give new meaning to convenience and choice. But before you visit your favorite boutique on the Net, take care to make your cyber-shopping experience safe.

THE BASICS

Think security, starting with your connection -- the way your computer connects through telephone wires to contact the Internet -- and your browser -- the software that acts like a telephone to receive information on the Internet.

Unsecured information sent over the Internet can be intercepted. That's why you should consider a secure browser, which will encrypt or scramble purchase information. Use a secure browser that complies with industry standards, such as Secure Sockets Layer (SSL) or Secure Hypertext Transfer Protocol (S-HTTP). These often are included with Internet connection services. The credit and charge card industry is working on an enhanced level of security using Secured Electronic Transactions (SET). SET protocol provides a highly encrypted communication between card issuers, merchants and card members.

If you don't have encryption software to assure the security of your transaction, consider calling the company's 800 number, faxing your order, or paying by check or money order.

Shop with companies you know. If you'd like to try a new merchant, ask for a paper catalog or brochure to get a better idea of their merchandise and services. Determine the company's refund and return policies before you place an order.

Never give out your Internet password.

Be original when creating your password(s). Consider using a combination of numbers, letters, and symbols, or use a phrase to remember it. For example: UR2G$48* -- "You are to give money for eight stars."

Avoid using established numbers for your password, such as your house number, birth date, or a portion of your telephone or Social Security numbers. It's a good idea to use different passwords to access specific areas on the Internet, such as the World Wide Web.

Be cautious if you're asked to supply personal information to conduct a transaction, such as your Social Security number. It's rarely necessary and should raise a red flag. The Internet provides a valuable information service for consumers. But some con artists who have used telemarketing, infomercials, newspapers, magazines, and the mail to attract consumers are turning to the Internet and online services to promote their scams.

Pay close attention to the information you're entering when you place an order. For example, an additional keystroke could get you 10 shirts when you wanted only one. Check to make sure the shipping charge is acceptable to you and all charges are calculated correctly.

Make a note of the company's shipping time. If you need the merchandise earlier, ask if your order can be "expressed" for an additional fee.

The same laws that protect you when you shop by phone or mail apply when you shop in cyberspace: Under the law, a company should ship your order within the time stated in its ads. If no time is promised, the company should ship your order within 30 days after receiving it, or give you an "option notice." This notice gives you the choice of agreeing to the delay or canceling your order and receiving a prompt refund.
There is one exception to the 30-day rule. If a company doesn't promise a shipping time, and you are applying for credit to pay for your purchase, the company has 50 days after receiving your order to ship.

Should you decide to pay by credit or charge card, your transaction will be protected by the Fair Credit Billing Act. Some cards may provide additional warranty or purchase protection benefits. If you're not comfortable entering your credit or charge card account number, call it into the company's 800 number, or fax it.

Print out a copy of your order and confirmation number for your records.

The Fair Credit Billing Act

Whether you're buying online, by phone, mail, or in person at a store, using your credit or charge card to pay offers some protections.

Errors...

If you find a billing error on your monthly credit or charge card statement, you may dispute the charge and withhold payment in that amount while the error is in dispute. The error might be a charge for the wrong amount, for something you didn't accept, or for something that wasn't delivered as agreed.

To Dispute a Charge...

◆Write to the creditor at the special address indicated on the monthly statement for "billing inquiries." Include your name, address, and credit or charge card number, and describe the billing error.

◆Send your letter as soon as possible. It must reach the creditor within 60 days after the first bill containing the error was mailed to you.

The creditor must acknowledge your complaint in writing within 30 days of receiving it, unless the problem has already been resolved. The creditor must resolve the dispute within two complete billing cycles -- but not more than 90 days -- after receiving your letter.

Unauthorized Charges...

If your credit or charge card is used without your authorization, you can be held liable for up to $50 per account. If you report the loss of your card before it is used, you are not liable for any unauthorized charges. See our Brochure on Fair Credit Billing.

FOR MORE INFORMATION

The Federal Trade Commission (FTC) publishes brochures on topics such as: automobiles, credit, products and services, and telemarketing. You can contact the FTC at: Consumer Response Center, Federal Trade Commission, Washington, D.C. 20580, 202-326-2222 , TDD: 202-326-2502, http://www.ftc.gov.

The Indiana Department of Financial Institutions, Division of Consumer Credit has many other credit related brochures available, such as:

- Answers to Credit Problems
- Applying for Credit
- At Home Shopping Rights
- Bankruptcy Facts
- Buried in Debt
- Car Financing Scams
- Charge Card Fraud
- Choosing A Credit Card
- Co-Signing
- Credit and Divorce
- Credit and Older Consumers
- Deep in Debt?
- Equal Credit Opportunity
- Fair Credit Reporting
- Fair Debt Collection
- Gold Cards
- Hang up on Fraud
- High Rate Mortgages
- Home Equity Credit Lines
- How to Avoid Bankruptcy
- Indiana Uniform Consumer Credit Code
- Look Before you Lease
- Mortgage Loans
- Repossession
- Reverse Mortgage Loans
- Rule of 78s – What is it?
- Scoring for Credit
- Shopping for Credit
- Using Credit Cards
- Variable Rate Credit
- What is a Budget?
- What is the DFI?

Call our toll-free number or write to the address on the cover for a copy of any of the brochures listed or for further consumer credit information. You can also access information at our web site on the Internet: http://www.dfi.state.in.us, then click on Consumer Credit.

CYBER-SHOPPING

DEPARTMENT OF FINANCIAL INSTITUTIONS
Consumer Credit Division
402 West Washington Street, Room W066
Indianapolis, Indiana 46204
317-232-3955
1-800-382-4880
Web Site http://www.dfi.state.in.us

As debit cards become increasingly popular, strains are appearing among customers, merchants, and banks.

The problems range from difficulties when the cards are lost or stolen to complaints from merchants that the fees to accept these cards are too high.

Not All Plastic is Created Equal

New car rental rules represent the first case in which debit cards cannot be used in the same way as credit cards. The big car rental companies, including Hertz and Avis, have recently stopped letting people rent cars using just a Visa Check card or the similar Master Money card from MasterCard. The card companies, and the banks that issue these cards - known as debit cards - are furious. And so are some customers.

For years, the car rental companies have used possession of a credit card as a crude way to weed out potentially risky renters, just as they have usually ruled out renters under the age of 25. But this test does not work with debit cards because banks will now give them to nearly any one with a bank account.

Charges on debit cards, which go under many names, come directly out of a consumer's checking account almost immediately rather than appearing on a monthly credit card statement. In contrast to using a credit card, which the debit card physically resembles, no loan is involved in the transaction.
Debit cards "provide no qualification of credit-worthiness," a Hertz spokesperson said. Car rental companies believe they are entitled to a certain level of confidence because in car rental, unlike almost any other business, the customer is given total control of a vehicle with an approximate value of $20,000.

The rental car companies are requiring a customer with only a debit card to follow the same procedures as someone who pays cash to rent a car. That involves making an application several weeks in advance and leaving a substantial deposit.

Higher Fees?

The new debit cards have become more popular because they are easier to use and more widely accepted than those that require personal identification numbers. Moreover, for the tens of millions of Americans who do not qualify for a credit card, the cards are their first opportunity to put a card with a MasterCard or Visa label in their wallets.

Until recently, such cards also provided the easiest way for such individuals, many of whom have had financial troubles, to rent a car or buy merchandise over the phone.
Banks like the debit cards because transactions on them are less costly to process than paper checks. Also, some banks charge customers a fee for the cards. And for the MasterCard and Visa versions, banks receive a fee from merchants of about one percent of the purchase price. Retailers, though, have become increasingly unhappy about the growth of these debit cards precisely because they do not want to pay the fee.

Confusingly, a single card can have both a Visa or MasterCard logo and the mark of an automated teller machine network like NYCE or MAC. If a signature is used, rather than a personal identification number, the fee paid by the merchant is higher.

The credit card companies say the higher fee is justified because of the greater risk. Even though both types of transactions involve electronic verification of the amount of money in the consumer's checking account, the card companies say their experience has been that the signature method results in more overdrafts.

For consumers, the debit cards also carry a little more risk. If the card is stolen, a thief can go on a spending spree with the money in the customer's checking account.

Federal law limits liability to $50 if the cardholder notifies the bank within two days of discovering the missing card. But the bank has up to 20 days to put the money back into the checking account.

See our Brochure on Credit and ATM Cards.

The Indiana Department of Financial Institutions, Division of Consumer Credit has many other credit related brochures available, such as:

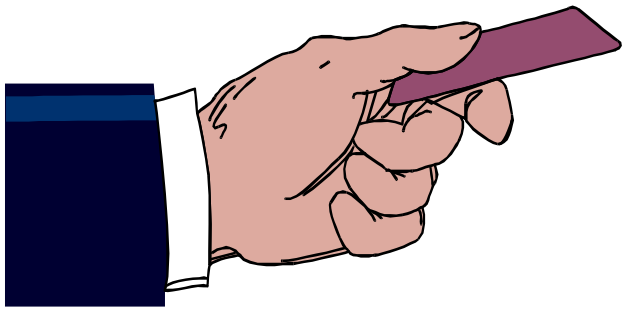
- Answers to Credit Problems
- Applying for Credit
- At Home Shopping Rights
- Bankruptcy Facts
- Buried in Debt
- Car Financing Scams
- Charge Card Fraud
- Choosing A Credit Card
- Co-Signing
- Credit and Divorce
- Credit and Older Consumers
- Deep in Debt?
- Equal Credit Opportunity
- Fair Credit Reporting
- Fair Debt Collection
- Gold Cards
- Hang up on Fraud
- High Rate Mortgages
- Home Equity Credit Lines
- How to Avoid Bankruptcy
- Indiana Uniform Consumer Credit Code
- Look Before you Lease
- Mortgage Loans
- Repossession
- Reverse Mortgage Loans
- Rule of 78s – What is it?
- Scoring for Credit
- Shopping for Credit
- Using Credit Cards
- Variable Rate Credit
- What is a Budget?
- What is the DFI?

Call our toll-free number or write to the address on the cover for a copy of any of the brochures listed or for further consumer credit information. You can also access information at our web site on the Internet: http://www.dfi.state.in.us, then click on Consumer Credit.

DEBIT

VS.

CREDIT CARDS



DEPARTMENT OF FINANCIAL INSTITUTIONS
Consumer Credit Division
402 West Washington Street, Room W066
Indianapolis, Indiana 46204
317-232-3955
1-800-382-4880
Web Site http://www.dfi.state.in.us

FAST FACTS

◆ Electronic banking, also known as electronic fund transfer (EFT), uses computer and electronic technology as a substitute for checks and other paper transactions.

◆ An access device is a means of gaining access to your account, such as a card or a code, for the purpose of initiating EFTs. Most institutions use a personal identification number (PIN) for this purpose.

◆ Take care of your EFT card. Know where it is at all times and report its loss as soon as possible.

◆ Choose a PIN different from your address, telephone number, social security number, or birth date.

◆ Keep and compare your EFT receipts with your periodic statements so that you can find and promptly report errors and unauthorized transfers. Prompt reporting is necessary to limit your liability for these problems

To most of us, electronic banking means having 24-hour access to cash through an automated teller machine (ATM) or having our paychecks deposited directly into our checking or savings accounts. But electronic banking offers several other services that you may find useful.

This brochure lists types of consumer transactions that are covered under the federal Electronic Fund Transfer Act (EFT Act), discusses the information financial institutions must disclose, explains what you can do if you find errors on your monthly statements, discusses your liability if your ATM card is lost or stolen, and describes your limited stop-payment privileges.

ELECTRONIC FUND TRANSFERS

Electronic banking, also known as electronic fund transfer (EFT), uses computer and electronic technology as a substitute for checks and other paper transactions. Because EFTs are so convenient, you may wish to know the full range of their services.

Automated Teller Machines or 24-hour Tellers are electronic terminals that permit you to bank at almost any time of the day or night. To withdraw cash, make deposits, or transfer funds between accounts, you generally insert a special ATM card and enter your personal identification number (PIN).

Direct Deposits or Withdrawals allow you to authorize specific deposits such as paychecks and social security checks to go directly to your account on a regular basis. You also can arrange to have recurring bills, such as insurance premiums and utility bills, paid automatically. This service applies only if you authorize transactions in advance.

Pay-by-Phone Systems permit you to telephone your bank (or other financial institutions) with instructions to pay certain bills or to transfer funds between accounts. You must have an agreement in advance with the financial institution to make such transfers.

Point-of-Sale Transfers allow you to pay for retail purchases with an EFT (or "debit") card. This is similar to using a credit card, but with one important exception -- the money for the purchase is transferred immediately (or soon thereafter) from your bank account to the store's account. Both MasterCard and Visa, among others, offer debit cards that can be used at participating retailers, and an increasing number of merchants are accepting this type of payment. For example, these transfers are becoming more common at grocery stores, oil companies, and convenience stores. However, because point of sale transfers are still relatively new, they might not yet be widely available at retailers in your region of the country.

DISCLOSURES

The best way to understand your legal rights and responsibilities regarding your EFT account is to read the documents you receive from the financial institution that issued you the "access device." An access device is a card, code, or other means of gaining access to your account for the purpose of initiating electronic fund transfers. The means may vary from institution to institution, but most use a PIN for this purpose. This unique number should be known only to you and to select employees of the financial institution.

Before you contract for EFT services or make your first electronic transfer, the institution is required to disclose to you the following information in a form you can keep.

- A summary of your liability for unauthorized transfers.
- The telephone number and address of the person to be notified when you believe that an unauthorized transfer has been or may be made, along with a statement of the institution's "business days." This information will tell you the number of days you have to report suspected unauthorized transfers.
- The type of transfers you can make, the amount of any charges for transfers, and any limitations on the frequency and dollar amount of transfers.
- A summary of your right to receive documentation of transfers, of your right to stop payment on a pre-authorized transfer, and the procedures to follow to stop payment.
- A notice describing the procedures you must follow to report an error on a receipt for an EFT, how to request more information about a transfer listed on your statement, and the time period in which you must make your report.
- A summary of the institution's liability to you if it fails to make or stop certain transactions.
- Circumstances under which the institution will disclose information to third parties concerning your account.

In addition to these disclosures, you will receive for most transactions two other types of important papers -- terminal receipts and periodic statements. (Separate rules apply to passbook accounts from which pre-authorized transfers are drawn. Your contract for that account is the best source of information about those rules.) You are entitled to a terminal receipt each time you initiate an electronic transfer, whether you use an ATM or make a point-of-sale electronic transfer. Among other things, the receipt must show the date and the amount of the transfer and the type of the transfer, such as "transfer from savings to checking." When you make a point-of-sale transfer, you probably will get your terminal receipt from the salesperson. If you make a withdrawal from a cash-dispensing machine that cannot issue receipts, the institution is required to mail you a receipt on the next business day following the transfer.

New provisions to the EFTA, effective immediately; compliance mandatory as of October 1, 2001, require ATM operators that impose a fee for providing electronic fund transfer services to post a notice in a prominent and conspicuous location on or at the ATM. The operator must also disclose that a fee will be imposed and the amount of the fee, either on the screen of the machine or on a paper notice, before the consumer is committed to completing the transaction. In addition, when the consumer contracts for an electronic fund transfer service, financial institutions are required to provide initial disclosures, including a notice that a fee may be imposed for electronic fund transfers initiated at an ATM operated by another entity.

You also are entitled to a periodic statement for each statement cycle in which an electronic transfer is made. This statement must show, among other things, the amount of any transfer, the date it was credited or debited to your account, the type of transfer and type of account(s) to or from which funds were transferred, and the address and telephone number to be used for inquiries. You are entitled to a quarterly statement even if you made no electronic transfers within that quarter.

Keep and compare your EFT receipts with your periodic statements each month in the same way you compare your credit card invoices with your monthly credit card statement or your checks against your monthly bank statements. Doing so will enable you to make the best use of your rights under federal law to dispute errors and avoid liability for unauthorized transfers.

ERRORS

You have 60 days from the date a problem or error appears on your periodic statements or terminal receipt to notify your financial institution. The best way to protect yourself in the event of an error (or a lost or stolen ATM or EFT card) is to notify the issuer by certified letter, return receipt requested, so you can prove that the institution received your letter. Keep a copy of the letter you send for your records.

After notification about an error on your statement, the institution has 10 business days to investigate and tell you the results. If the institution needs more time, it may take up to 45 days to complete the investigation -- but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error is found, the institution may take the money back, if it sends you a written explanation.

If you fail to notify the institution of the error within 60 days, you may have little recourse. Under federal law, the institution has no obligation to conduct an investigation if you have missed the 60-day deadline.

If your failure to notify the institution within the time periods allowed was due to an extenuating circumstance, such as lengthy travel or illness, the issuer must extend the time period for notification to what is reasonable. Also, if state law or your contract imposes lower liability limits, those lower limits apply instead of the limits in the federal EFT Act.

After reporting the loss or theft of your ATM card, you are not liable for additional unauthorized transfers that may be made. Because these unauthorized transfers may appear on your statements, however, you should carefully review each statement you receive after you report the loss or theft. If the statement shows transfers that you did not make or that you need more information about, contact the institution immediately, using the special procedures provided for reporting errors.

LIMITED STOP-PAYMENT PRIVILEGES

When you use an electronic fund transfer, the EFT Act does not give you the right to stop payment. If your purchase is defective or if your order is not delivered, it is up to you to resolve the problem with the seller and get your money back -- just as if you had paid cash.

There is one situation, however, in which you can stop payment. If you have arranged regular payments out of your account to third parties, such as life insurance companies, you can stop payment if you notify your institution at least three business days before the scheduled transfer. The notice may be oral or written, but the institution may require a written follow-up to be made within 14 days of the oral notice. Your failure to provide the written follow-up ends the institution's responsibility to stop payment. This right to stop payment does not apply to mortgage or loan payments you owe to the institution that issued the EFT access device.

Although federal law provides only limited rights to stop payment, individual financial institutions may offer more rights or state laws may require them. If this feature is important to you, you may want to shop around to be sure you are getting the best "stop payment" terms available.

SUGGESTIONS

If you decide to become an EFT user, remember the following precautions.

◆ Take care of your EFT card. Know where it is at all times and report its loss as soon as possible.

◆ Choose a PIN different from your address, telephone number, social security number, or birth date. Choosing a different number will make it more difficult for a thief to use your EFT card.

◆ Keep and compare your EFT receipts with your periodic statements so that you can find and promptly report errors and unauthorized transfers.

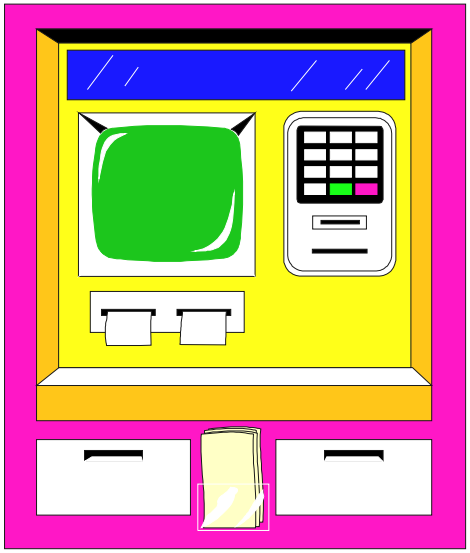
If you believe the institution that issued your EFT access device has failed to fulfill its responsibilities to you under the EFT Act, in addition to informing the issuer, you may wish to complaint to the federal agency that has enforcement jurisdiction over that issuer

---

The Indiana Department of Financial Institutions, Division of Consumer Credit has many other credit related brochures available, such as:

Answers to Credit Problems
Applying for Credit
At Home Shopping Rights
Bankruptcy Facts
Buried in Debt
Car Financing Scams
Charge Card Fraud
Choosing A Credit Card
Co-Signing
Credit and Divorce
Credit and Older Consumers
Deep in Debt?
Equal Credit Opportunity
Fair Credit Reporting
Fair Debt Collection
Gold Cards
Hang up on Fraud
High Rate Mortgages
Home Equity Credit Lines
How to Avoid Bankruptcy
Indiana Uniform Consumer Credit Code
Look Before you Lease
Mortgage Loans
Repossession
Reverse Mortgage Loans
Rule of 78s – What is it?
Scoring for Credit
Shopping for Credit
Using Credit Cards
Variable Rate Credit
What is a Budget?
What is the DFI?

ELECTRONIC BANKING



DEPARTMENT OF FINANCIAL INSTITUTIONS
Consumer Credit Division
402 West Washington Street, Room W066
Indianapolis, Indiana 46204
317-232-3955
1-800-382-4880
Web Site http://www.dfi.state.in.us

SWINDLERS HAVE COMPUTERS TOO

Cyberspace is a vast new territory for unscrupulous marketers. The National Fraud Information Center reports that while fraudulent commercial activity on the Internet is not yet a major problem, as use expands, there is sure to be a major increase in deceptive and misleading promotions.

Swindlers are attracted to the Internet because they can reach thousands of consumers inexpensively, quickly and anonymously. Few restrictions exist on the Internet, making it easy to place deceptive or misleading information online.

Judging the accuracy and reliability of online information is a major challenge for consumers. False or misleading information related to personal finance or health issues, for example, could lead to serious consequences for unsuspecting consumers.

FRAUD ON THE NET

The Federal Trade Commission began investigating fraud on the Internet in 1994. They found that the same kinds of fraud that occur in other places also surface on the Net. Electronic bulletin boards, chat groups, and e-mail networks are fertile grounds for old-fashioned scams that apply false advertising claims and deceptive marketing practices.

Electronic Bulletin Boards provide new sources of information to Internet users telling about products, services, and investment opportunities. At the same time these electronic bulletin boards can carry false and misleading ads for products that promise quick solutions to desirable goals such as weight loss or easy business success. The plan is to have you use your PC to make plenty of money in a short period of time.

Discussion groups or chat forums often form on the Internet where interested parties can exchange information on specific topic areas. These chat rooms sometimes appear to be open discussion when they are sales pitches in disguise. In some cases, people involved in the discussion may have financial ties to businesses that sell products or services related to the topic area. This disguised advertising may not be obvious to the consumer.

E-mail scams involve individuals or companies intentionally misleading consumers or using deceptive marketing practices to gain the consumer's interest in their product. For example, the use of a particular product is advertised to cure a specific medical condition. These are the same health, diet, and fitness schemes that occur in other marketplace venues, such as mail-order and telemarketing schemes. Other types of e-mail scams involve the sale of worthless products, phony credit repair companies, term paper peddlers, expensive work-at-home deals, psychic hotlines, and deceptive promises related to contests, awards, sweepstakes, and free gifts.

Pyramid or Ponzi schemes and chain letters are well suited to the Internet because they entice investors with the promise of quick profits using a home computer. Investors make money by recruiting new investors. The problem is that soon the program runs out of new investors and most players lose the money they invested. Chain letter schemes ask participants to send money to the names at the top of a list with the promise that they will eventually receive thousands of dollars when their names come to the top. Unsuspecting persons lose money every day on this illegal practice.

Risk-free investment opportunities on the Internet offer fraudulent technological and exotic investments such as wireless cable, bogus securities, or worthless land. These investments promise to yield far greater returns than do commonly available investment products. The term "risk-free" is highly misleading. Few consumers get their money back, much less make a profit.

Pump and Dump stock manipulations on the Internet encourage investors to buy a particular stock, which is usually little known and low cost. The promoters may even advertise that they have inside information. They make their profit when consumers buy the stock, or pump up the price and the promoters then promptly sell, or dump their shares and the stock prices immediately fall. This scheme can also work in reverse; a short seller makes a profit when the price of the stock goes down.

PROBLEMS WITH INTERNET TRANSACTIONS

Two problems with Internet sales transactions are personal data privacy and verification that both buyers and sellers are authentic. Many consumers are concerned about the confidentiality of their personal financial information on the Web, with good reason. When you make a purchase on the Internet, your credit card number could fall into the wrong hands. Personal data can be collected and organized into database files. When you become a part of an on-line service, your personal data can be available to everyone in that system. While it is unlikely that reputable merchants would deliberately sell your data to others, their database may be tempting targets for hackers.

Verification that consumers are who they say they are can be solved by an electronic equivalent of a signature or a driver's license. A software product currently used by merchants, banks, and brokerage houses tells who the user is and what privileges he or she has. There is a growing interest in credit card payment systems that would safeguard credit card purchases on the Net. Encryption software can scramble your personal information so that it can be read only by the sender and the receiver. The problem remains that personal data might still be available to certain employees or hackers.

Experts urge consumers to avoid dealing with Internet sites they are not familiar with. Even when dealing with a well-known business, call the business directly to verify that the site exists. It continues to be a risky business to give personal information, including address and phone number, credit card numbers, social security numbers, and bank account numbers on the Internet.

PROTECTION AGAINST INTERNET FRAUD

Most people find it hard to believe that they could become victims of fraud, but one should never underestimate the ingenuity of swindlers who make money by misleading others. State and federal laws and agencies have limited capacity to protect consumers from fraud on the Internet. The savvy consumer must stay alert to the possibility of fraud. The National Fraud Information Center offers the following suggestions for side-stepping fraud on the Internet:

Never reveal checking account numbers, credit card numbers, or other personal financial data at any Web site or online service location -- unless you are sure you know where this information will be directed.

When you subscribe to an on-line service you may be asked for credit card information. When you enter any interactive service site however, beware of con artists who may ask you to "confirm" your enrollment in the service by disclosing

passwords or the credit card account number used to subscribe.

Use the same common sense you would exercise with any direct or telephone credit card purchase. A flashy professional Internet Web site does not guarantee that the sponsor is legitimate. Know the company with which you plan to do business.

Report anything you see on the Internet that you suspect might be fraudulent. The National Fraud Information Center's toll-free number is 1-800-876-7060. Their mailing address is P.O. Box 65868, Washington, D.C. 20035. Their Web address is http://www.fraud.org

Your state Office of the Attorney General is empowered to investigate consumer complaints, including Internet complaints. They can give you information about any problems or concerns they have encountered with the business.

The Better Business Bureau can tell you if there have been any complaints or inquiries about a business and how it was resolved. Some online advertisements will have a blue-seal that you can click on to connect to the Better Business Bureau for a report on the advertiser's track record. The online Web site for the BBB is http://www.bbbonline.org

The Federal Trade Commission enforces several consumer protection laws that are relevant to computer transactions, such as false advertising and consumer credit. Suspicious actions on the Web, when reported to the National Fraud Information Center, are shared with the Federal Trade Commission and the National Association of Attorneys General. In this way, consumers join with state and federal agencies in actions to curtail fraud on the Internet.

Although many regulations and agencies have been established to protect consumers from fraud, the principle of let the buyer beware remains the consumer's best protection. Legal protections are limited, fraudulent activities flourish, and once money is lost in a fraudulent scheme the chances of getting it back are extremely small. Awareness of the possibility of fraud is your first line of defense.

The Indiana Department of Financial Institutions, Division of Consumer Credit has many other credit related brochures available. Call our toll-free number or write to the address on the cover for a copy of any of our listed or for further consumer credit information. You can also access information at our web site on the Internet: http://www.dfi.state.in.us, then click on Consumer Credit.

FRAUD ON THE INTERNET

DEPARTMENT OF FINANCIAL INSTITUTIONS
Consumer Credit Division
402 West Washington Street, Room W066
Indianapolis, Indiana 46204
317-232-3955
1-800-382-4880
Web Site http://www.dfi.state.in.us